UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/613,004	07/10/2000	Richard D. Haney	PRC-001	9157

26717 7590 11/30/2004

RONALD CRAIG FISH, A LAW CORPORATION
PO BOX 820
LOS GATOS, CA 95032

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/613,004	HANEY, RICHARD D.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on June 17, 2004. Original application contained Claims 1-5. Applicant cancelled Claims 1-5 and added new Claims 6-10. The amendment filed have been entered and made of record. Presently pending claims are 6-10.

Claim Rejections - 35 USC § 112

Claim 6 recites the limitation "said AlterWAN" in limitation 'c' line 17. There is insufficient antecedent basis for this limitation in the claim.

Response to Arguments

Applicant's arguments filed on June 17, 2004 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-5 applicants argued that the cited prior art (CPA) [Provino (U.S. Patent No. 6,557,037)] does not teach, " *when packet is generated, it is routed across the internet over a preplanned, pretested, low hop count, high bandwidth data path by specially*

selected ISP/ISX providers who have been selected and whose routers are configured to make sure packets get routed specially over this high bandwidth, low hop count path"

This is not found persuasive. CPA clearly teaches system and method that provides a connection between a virtual private network (15) and external units via the Internet (14). The connection between the external units is made using a service provider (11). The virtual private network has a firewall (30) and internal servers (31) for secondary addresses and name addresses.

The system and method of CPA provide wide area networking services to clients with many locations among which data, especially high volumes of data, must be sent, and providing an improved system for communications using the Internet.

As a result, CPA does implement and teach a system and method uses the Internet as a WAN backbone to help decrease the costs of data transport while not suffering from the latency, privacy and bandwidth availability problems.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that CPA does teach or suggest the subject matter recited in independent Claims 6-10. Accordingly, rejections for claims 6-10 are respectfully maintained.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 6-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino (U.S. Patent No. 6,557,037).

3. With respect to claim 6, Provino teaches a private, secure wide area network between a source site and a destination site using the internet as a backbone, comprising:

a first dedicated local loop connection providing a signal path to a router of a source ISX/ISP provider of Internet access (see col. 3, lines 37-62; col. 4, lines 61-67 to col. 5, lines 1-17);

a source router located at a source site and having a channel service unit having an output coupled to said first dedicated local loop connection (see col. 3, lines 59-67 to col. 4, lines 1-23);

a source firewall circuit located at a source site and having a first port for coupling directly or through a local area network to one or more computers or other devices at said source site for which communication over said private, secure wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local

area network, said source firewall functioning to encapsulate any Internet Protocol packets hereafter IP packets transmitted from said first computer or other device which have a destination Internet Protocol address (hereafter IP address) which is one of a set of IP addresses of computers or other devices at a destination site, said encapsulation being into the payload sections of IP packets having as their destination address the IP address of a firewall at said destination site and for encrypting said payload sections of said AlterWAN packets using any encryption method having a key, and transmitting said AlterWAN packets to said source router, where IP packets having as their destination address the IP address of a computer or other device at either said source site or said destination site and having an encrypted IP packet transmitted from a computer or other device at said source site or said destination site as a payload being defined and hereafter referred to as AlterWAN packets, but for not encapsulating into AlterWAN packets any IP packets transmitted by said first computer or other device which do not have as their destination address an IP address which is one of said IP addresses of computers or other devices at said destination site, and for receiving incoming IP packets from various sources including computers and devices at said destination site via said source router and for recognizing AlterWAN packets among these IP packets and decrypting the payloads of said AlterWAN packets using the same encryption method and key or keys that were used to encrypt the AlterWAN packets to recover said IP packets that were encapsulated in said AlterWAN packets and transmitting at least said recovered IP packets to said one or more computers or devices at said source site (see col. 9, lines 46-67 to col. 10, lines 1-44);

one or more routers of other participating ISX/ISP providers of internet services besides said source ISX/ISP provider including a router at an endpoint participating ISX/ISP provider,

said routers of said source and endpoint ISX/ISP providers and said other participating ISX/ISP providers functioning to implement a predetermined private tunnel data path for said AlterWAN packets coupling a router of said source ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP providers and said other ISX/ISP providers being providers of Internet services who have contracted to provide and who have been pretested to verify that they do in fact provide a low hop count portion of a data path between said source site and said destination site for said AlterWAN packets with an average available bandwidth along said portion of said data path travelled by said AlterWAN packet which each ISX/ISP provider provides which substantially exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site(see col. 9, lines 32-67 to col. 10, lines 1-12);

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated local loop connection to said router of said endpoint ISX/ISP provider a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a one or more computers or devices for which communication across said private, secure wide area network is desired, said destination firewall functioning to encapsulate into the payload sections of AlterWAN packets IP packets transmitted from said one or more computers or devices at said destination site and having as their destination addresses an IP address of said one or more computers or devices at said source site, and functioning to encrypt the payloads of said

AlterWAN packets and transmit said AlterWAN packets to said destination router, but for not encapsulating into AlterWAN packets any IP packets transmitted from said one or more computers or devices at said destination site which do not have as their destination address an IP address of said one or more computers or devices at said source site, and for receiving IP packets from various sources including said one or more computers or devices at said source site via said destination router, and functioning to recognize AlterWAN packets among said received IP packets and decrypt the payload sections of said AlterWAN packets to recover the original IP packets using the same encryption protocol used by said source firewall to encrypt said payload sections of said AlterWAN packets and the same key or keys used by said source firewall and transmitting at least the decrypted IP packets recovered from AlterWAN packet to said one or more computers pr devices at said destination site (see col. 1, lines 38-45; col. 3, lines 59-67 to col. 4, lines 1-22, and col. 9, lines 46-67 to col. 10, lines 1-44; col. 15, lines 21-57).

4. With respect to claim 7, Provino teaches process for sending AlterWAN data packets securely between a computer at a source site and a computer at a destination site so as to implement a Wide Area Network between said source and destination sites of a customer using the internet as a backbone but which is private and which only said customer can use while simultaneously launching non-AlterWAN packets into a normal internet traffic routing data path (see abstract; Fig. 1), comprising the steps:

receiving at a source firewall incoming Internet Protocol packets (hereafter IP packets) from computers at a source site of a customer, some of said IP packets having as their destination addresses an Internet Protocol address (hereafter IP address) of a computer at a destination site of said customer (see col. 8, lines 58-67 to col. 9, lines 1-31),

at said source firewall, comparing the destination address in each said received IP packet to an IP address of a computer at said destination site of said customer, and if an IP packet has as its destination address the IP address of a computer at said destination site, concluding said IP packet is an AlterWAN packet payload which needs to be transmitted via a virtual private network over the internet to said computer at said destination site, but if said destination address of said received IP packet is not an IP address of a computer at said destination site, concluding said IP packet is not an AlterWAN payload packet and needs to be routed as any other IP packet would be routed if a received IP packet is an AlterWAN payload packet, encapsulating said AlterWAN payload packet into the payload section of an IP packet having as its destination address the IP address of a firewall at the destination end of said virtual private network (hereafter referred to as AlterWAN packet) and encrypting at said source firewall the payload portion of said AlterWAN packet using any encryption algorithm having a key which same encryption algorithm and key can be used by a firewall at said destination site to recover said AlterWAN payload packet, and forwarding said AlterWAN packet to a source router(see col. 10, lines 13-44),

if a received IP packet is not an AlterWAN payload packet, forwarding said received IP packet which is not an AlterWAN payload packet (hereafter referred to as a non-AlterWAN

packet) to said source router without encapsulating said non-AlterWAN packet into an AlterWAN packet (see col. 13,lines 26-53),

at said source router, converting both said AlterWAN packets and said non AlterWAN packets into signals suitable for transmission on a dedicated local loop connection coupling said source router to a specially selected source participating ISX/ISP provider and transmitting said signals to said specially selected source participating ISX/ISP provider, said specially selected source participating ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop-count data paths to next participating ISX/ISP provider in said virtual private network (see col. 4, lines 50-67 to col. 5, lines 1-17) or because the routing tables of the router of said specially selected source participating ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said virtual private network and wherein said source participating ISX/ISP provider and all other participating ISX/ISP providers whose routers route AlterWAN packets have contracted to provide a data path for said AlterWAN packets with an average available bandwidth which exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site of said customer *(see col. 4, lines 50-67 to col. 5, lines 1-17).*

5. With respect to claim 8, Provino teaches an apparatus comprising:

a dedicated data path for coupling signals to a specially selected first participating ISX/ISP provider of Internet access (see col. 3, lines 37-62; col. 4, lines 61-67 to col. 5, lines 1-17),

a first firewall circuit having a first port for coupling directly or through a local

area network to one or more devices for which communication over a private wide area network between a customer's source site and destination site using the internet as a backbone is desired, and having a second pod, said firewall functioning to use the destination addresses in the headers of each packet received from one or more devices at said source site to distinguish between conventional packets and AlterWAN payload packets, where AlterWAN payload packets are packets addressed to devices at said destination site or said source site, and wherein a computer at said destination site is coupled to a computer at said source site via a second firewall circuit and a virtual private network tunnel through a public wide area network such as the internet terminating at said source site at said first firewall circuit and terminating at said destination site at said second firewall circuit, and wherein conventional packets are packets which are not addressed to devices at said destination site said first firewall circuit functioning to encapsulate said AlterWAN payload packets in the payload section of AlterWAN packets which are addressed to said second firewall circuit at said destination end of said virtual private network tunnel, and further functioning to encrypt the payloads of AlterWAN packets using one or more predetermined keys and an encryption algorithm, and said first firewall circuit further functioning to distinguish between incoming AlterWAN packets and conventional packets by comparing the destination addresses thereof to the address of said first firewall circuit and concluding that any incoming packets addressed to said first firewall circuit are AlterWAN packet and all packets addressed to one or more computers at said source site coupled to said first firewall circuit are conventional packets, and to decrypt the payload sections of any incoming AlterWAN packets using the same encryption algorithm and one or more predetermined keys which were used to encrypt the AlterWAN packets so as to recover the

encapsulated AlterWAN payload packet (see col. 9, lines 32-67 to col. 10, lines 1-44);

a source router having an input coupled to said second pod of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said router and channel service unit functioning to receive said AlterWAN packets and said conventional packets from said first firewall circuit and convert said packets into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN packets and conventional packets over said dedicated data path to said specially selected first participating ISX/ISP provider where said AlterWAN packets will be routed via said virtual private network tunnel and specially selected participating ISX/ISP providers to said second firewall and non-AlterWAN packets will be routed along paths on the internet other than said virtual private network tunnel and wherein said first participating ISX/SSP provider and all said other ISX/ISP providers are providers who have contracted to and do in fact provide data paths for AlterWAN packets which combine to form a low hop count data path with an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site (see col. 9, lines 32-67 to col. 10, lines 1-44; col. 15, lines 21-57).

6. With respect to claim 9, Provino teaches a method of designing and implementing a wide area network using the Internet as a backbone (see abstract; Fig. 1), comprising the steps:

1) selecting source and destination sites that have computers or other devices (hereafter referred to simply as computers) that need to be connected by a wide area network (see Fig. 1),

2) examining available ISX/ISP internet service providers that can route AlterWAN packets between said source and destination sites and selecting two or more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which AlterWAN packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made so as to minimize the number of hops on the internet the routers at participating ISX/ISP providers will cause AlterWAN packets to take while traveling between said source and destination sites and so as to guarantee that the average available bandwidth of the data paths along which said AlterWAN packets traveling between computers at said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites (see col. 9, lines 32-67 to col. 10, lines 1-44),

3) pretesting the ISX/ISP providers selected in step 2 by testing to verify the data path that an AlterWAN packets will take through the internet to verify that what the participating ISX/ISP providers promised to deliver will actually be delivered see (col. 9, lines 32-67 to col. 10, lines 1-44; col. 15, lines 21-57),

4) contracting with said participating ISX/ISP providers to provide routing of AlterWAN packets so as to minimize the number of hops on the internet said AlterWAN packets need to take in traveling between said source and destination sites and so as to guarantee that the average available bandwidth along data paths AlterWAN packets must traverse to travel between said source and destination sites is substantially greater than the worst case bandwidth

consumption of traffic between source and destination sites, and, if necessary, configuring data in routing tables of said participating ISX/ISP providers so as to minimize said number of hops and guarantee said bandwidth contracted for when routing AlterWAN packets see (Fig.1, and col. 9, lines 32-67 to col. 10, lines 1-44; col. 15, lines 21-57),

5) contracting to establish a first dedicated local loop connection between the output of a source router at which said signals appear and said source ISX/ISP provider in the group of ISX/ISP providers selected in step 2, said first dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets traveling between said source and destination sites (see Fig. 1),

6) contracting to provide a second dedicated local loop connection connecting the input of a destination router to said destination ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in A1terWAN packets traveling between said source and destination sites(see col. 10, lines 34-67 to col. 11, lines 1-45),

7) coupling an untrusted port of a source firewall/virtual private network circuit (hereafter referred to as the source firewall) to a source router and coupling a trusted pod of said source firewall to said device or devices at said source site and configuring said source firewall to examine the destination addresses of Internet Protocol packets (hereafter IP packets) received from said devices at said source site and encapsulate each IP packet having a destination address which is the Internet Protocol address (hereafter IP address) of any device at said destination site as a payload portion in a second IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of a

destination firewall/virtual private network circuit (hereafter referred to as the destination firewall) at said destination site and having the original IP packet as its payload with portions of said AlterWAN packet other than said payload section being referred to herein as an AlterWAN packet header, said source firewall also being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which do not have as their destination address the IP address of any device at said destination site (hereafter referred to as non AlterWAN packets), and configuring said source firewall to screen incoming IP packets so as to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted port of said source firewall and to strip off the AlterWAN packet headers and decrypt the payload portion of each said incoming AlterWAN packet to recover the original IP packet transmitted from said destination firewall using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets when they were transmitted from said destination firewall so as to recover the original IP packet transmitted to said destination firewall by a computer at said destination site, and for outputting said recovered original IP packet to said device or devices at said source site having the IP address which is the destination address of said original IP packet (see col. 10, lines 34-67 to col. 11, lines 1-45);

8) coupling a source router to receive said encrypted AlterWAN packets and non-encrypted non-AlterWAN packets from said untrusted port of said source firewall and to convert said AlterWAN and non-AlterWAN packets in a channel service unit to signals suitable for transmission over said first dedicated local loop connection to said source ISX/ISP provider;

9) providing a destination router at said destination site having a firewall port coupled to said untrusted port of said destination firewall and having a channel service unit coupled to said destination ISX/ISP provider via said second dedicated local loop connection and which is configured to receive from said second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packets and conventional non AlterWAN IP packets and converting said signals back into the original digital IP packet form and configuring said destination router to output said recovered downstream IP packets at said firewall port coupled to said untrusted port of said destination firewall, and said destination router configured to receive upstream AlterWAN packets and conventional non AlterWAN packets and convert both types of said packets into signals suitable for transmission on said second dedicated local loop connection coupling said destination router to said participating destination ISX/ISP provider in the group of participating ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection (see col. 13, lines 26-53),

10) providing a destination firewall having an untrusted pod coupled to said firewall pod of said destination router so as to receive said recovered digital IP packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered IP packets having as their destination address the IP address of said destination firewall untrusted pod and further configured to strip off the AlterWAN packet header of each said AlterWAN packet and decrypt the payload portion of each said AlterWAN packet using the same encryption algorithm and encryption key or keys that were used to encrypt the AlterWAN packet at said source firewall so as to recover the original IP packet encapsulated in each AlterWAN packet, and configuring said destination firewall to output the decrypted original IP packets at an output coupled to a device

or devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from a device or devices at said destination site and encapsulate each upstream IP packet addressed to any computer or other device at said source site as the payload portion of in another IP packet, hereafter referred to as an upstream AlterWAN packet (an AlterWAN packet traveling from said destination site toward said source site), said AlterWAN packet having as its destination address the IP address of said untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said upstream AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any non AlterWAN IP packets received from said device or devices at said destination site which do not have as their destination addresses an IP address of any device at said source site (hereafter referred to as conventional non AlterWAN packets), and said destination firewall configured to transmit said encrypted upstream AlterWAN packets and said conventional non AlterWAN packets to said destination router via said untrusted pod (see col. 9, lines 32-67 to col. 10, lines 1-44; col. 13, lines 26-53; col. 15, lines 21-57).

7. With respect to claim 10, Provino teaches private wide area network connecting a customer source site to a customer destination site and using the internet as a backbone (see abstract; Fig. 1), comprising:

a first dedicated data path coupled to a first participating ISX/ISP provider of Internet access (see col. 3, lines 37-62; col. 4,lines 61-67 to col. 5, lines 1-17);

a source router having a channel service unit having an output coupled to said first dedicated data path (see col. 3, lines 37-62; col. 4,lines 61-67 to col. 5, lines 1-17);

a source firewall circuit having a first port for coupling directly or through a local area network to one or more devices at a customer source site, and having an untrusted pod coupled to said source router directly or through a local area network, said untrusted port of said source firewall having an Internet Protocol address (hereafter IP address), said source firewall functioning to receive Internet Protocol packets (hereafter IP packets) from said one or more devices at said customer source site which are addressed to one or more devices at a customer destination site (hereafter AlterWAN payload packets) and other IP packets addressed to other locations on the internet (hereafter conventional IP packets), and for encapsulating said AlterWAN payload packets as the payload sections of IP packets addressed to an IP address of an untrusted port of a destination firewall at said customer destination site (hereafter outgoing A1terWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets using a first encryption method known to a destination firewall and using a key or key known to said destination firewall and which may be user definable, and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted port of said source firewall circuit, and decrypting the payload sections of any incoming IP packets having as their destination address the IP address of said untrusted port of said source firewall circuit (hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt them so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and

transmitting each recovered AlterWAN payload packet to a device at said customer source site to which said AlterWAN payload packet is addressed (see col. 9, lines 46-67 to col. 10, lines 1-44);

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement a low hop count data path in the form of a virtual private network tunnel through the internet coupling one or more devices at said customer source site to one or more computers at said customer destination site, said low hop count data path having an average available bandwidth which is substantially greater than the worst case bandwidth consumption of AlterWAN packets traveling between said customer source site and said customer destination site (see col. 9, lines 32-67 to col. 10, lines 1-12);

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated datapath to said router of said endpoint participating ISX/ISP provider (see col. 1, lines 38-45; col. 3, lines 59-67 to col. 4, lines 1-22);

a destination firewall circuit having an untrusted port having an IP address to which said outgoing AlterWAN packets are addressed, said untrusted port coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to one or more devices at said customer destination site, said destination firewall circuit functioning to receive IP packets from said one or more devices at said customer destination site which are addressed to one or more devices at said customer source site (hereafter AlterWAN payload packets) and functioning to receive other conventional IP packets, and for encapsulating said AlterWAN payload packets as the payload sections of AlterWAN

packets addressed to said IP address of an untrusted port of said source firewall circuit at said customer source site (hereafter outgoing AlterWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets using an encryption method known to said source firewall and a key or keys known to said source firewall and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted pod of said destination firewall circuit, and decrypting the payload sections of any incoming IP packets having as their destination address the IP address of said untrusted port of said destination firewall circuit (hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt said incoming AlterWAN packets so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to the device to which it is addressed at said customer destination site (see col. 9, lines 46-67 to col. 10, lines 1-44; col. 19, lines 21-57).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
November 27, 2004

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
11/4 2136